THOMSON REUTERS®

Are HIPAA Covered Entities and Business Associates Required to Have a Risk Analysis and a Risk Management Plan?

EBIA Weekly (March 7, 2024)

QUESTION: What is the difference between a HIPAA risk analysis and a risk management plan? Do covered entities and business associates need both?

ANSWER: HIPAA's security management process standard requires covered entities and business associates to have both a risk analysis and risk management plan. The risk analysis is required to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI). The risk analysis cannot be a simple "gap analysis" that identifies deficiencies in compliance programs, it must address all ePHI across the entire enterprise and identify deficiencies in compliance programs when compared to the HIPAA security rule. Based on the results of the risk analysis, the risk management plan is created to determine what safeguards need to be implemented to bring the identified risks and vulnerabilities to a reasonable level. The risk management plan should assign responsibilities, due dates, and status updates. Preferably, the risk management plan should have a one-to-one correlation with the risk analysis.

Covered entities and business associates are required to periodically update the mandatory risk analysis and risk management plan, to identify the level of risk that is acceptable. Generally, an evaluation should occur annually, but less frequent reviews may be appropriate depending on the organization. The risk analysis and risk management plan also should be reviewed each time an organization's security environment changes, e.g., if the entity has experienced a security breach or significant security incident.

In conducting its compliance audits, OCR regularly penalizes covered entities for failure to conduct an adequate risk analysis and create a risk management plan in accordance with HIPAA's documentation and record retention requirements. OCR has also found fault with covered entities and business associates that adopt "off-the-shelf" risk analyses or risk management plans; these documents must be tailored to each covered entity's or business associate's unique operating environment. HHS has an updated version of its interactive Security Risk Assessment Tool that highlights the importance of creating a risk management plan that remediates risks identified in the risk analysis by documenting a plan for improvement, assigning responsibilities, and tracking deadlines.

For more information, see EBIA's HIPAA Portability, Privacy & Security manual at Sections XX.C ("HIPAA Compliance Audits by OCR"), XX.D ("Resolution Agreements"), XXIX.E ("Developing Your Security Program"), XXIX.F ("Limiting Exposure Through 'Recognized Security Practices'"), XXX.B ("Administrative Safeguards"), and XXXI.E ("Problems Relating to HIPAA Security").

Contributing Editors: EBIA Staff.